УДК 343.98

СПОСОБЫ ПОДГОТОВКИ, СОВЕРШЕНИЯ И СОКРЫТИЯ ХИЩЕНИЙ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ: КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА

Д. И. Шнейдерова
преподаватель кафедры уголовного процесса и криминалистики
Могилевского института МВД (Беларусь)

Статья посвящена криминалистическому анализу способа совершения хищений в сфере оборота криптовалют как полноструктурного явления, включающего триаду способов подготовки, совершения и сокрытия преступлений. Автором обращается внимание, что правовое закрепление имущественного статуса криптовалют позволяет рассматривать их в механизме совершения различных видов хищений как предмет преступного посягательства, а также как средство реализации преступного умысла или сокрытия похищенных денежных средств, что влияет и на целевую направленность выбранного преступником способа совершения хищения. Среди способов приготовления автором выделяются подбор необходимых технических средств, вредоносного программного обеспечения для блокирования работы или удаленного шпионажа за устройством потерпевшего, прохождение предварительного обучения, сбор информации о лицах, в отношении которых планируется хищение, подбор соучастников и распределение ролей, выбор средств анонимизирования личности в сети Интернет. Способы совершения разделяются в зависимости от вида совершенного хищения и группируются как способы, относящиеся к вымогательству, мошенничеству, хищению путем модификации компьютерной информации. Способы сокрытия характеризуются комплексом действий по ликвидации или сокрытию электронно-цифровых следов, а также анонимизированию или выводу похищенных криптовалют и денежных средств.

Ключевые слова: *криптовалюта, криптокошелек, хищение, способ, сокрытие, подготовка, криминалистическая характеристика, мошенничество, вымогательство, модификация.*

Хищения, совершаемые с использованием компьютерных и телекоммуникационных технологий, составляют неотъемлемый и развивающийся сектор киберпреступлений, внедрение в который новых средств, способов и механизмов совершения преступлений находится в прямой зависимости от распространения и общедоступности продуктов информационно-технического прогресса. Одним из таких малоисследованных с точки зрения криминалистической науки, но достаточно распространенных среди представителей преступного мира продуктов выступает криптовалюта. Будучи объектом цифровой индустрии, лишенным видимой физической оболочки, криптовалюта за счет своего свойства обмениваться на денежные средства и иные материальные активы обладает определенной имущественной ценностью. Данное обстоятельство в совокупности с легализацией ее правового статуса Декретом Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» позволяет признавать криптовалюту не только средством совершения или сокрытия преступлений, но и предметом преступных посягательств против собственности [1].

Криминалистическое исследование криптовалют и их места в системе хищений базируется на криминалистической характеристике отдельных элементов механизма преступления, среди которых связующим звеном выступает способ совершения преступления. Анализ научной литературы показал, что существует несколько различных трактовок понятия «способ совершения преступления», однако все они в той или иной степени походят на определение, представленное Р. С. Белкиным, который под способом совершения преступления понимает совокупность действий, направленных на подготовку, совершение и сокрытие преступления, обусловленных условиями внешней среды и психофизическими свойствами личности преступника [2, с. 132].

А. С. Князьков отмечает, что понятие, предложенное Р. С. Белкиным, является собирательным и отражает сущность способа совершения преступления как полноструктурного образования, где объединены способы приготовления, совершения и сокрытия преступления. Однако следует согласиться с мнением автора, что не в каждой ситуации можно вести речь о наличии полноструктурного способа, поскольку практике известны случаи, когда умышленные преступления совершают спонтанно, без подготовки, или без сокрытия, либо без обоих указанных элементов, а в случае совершения преступлений по неосторожности нецелесообразно говорить о способах подготовки и совершения преступления в силу характера посягательства [3, с. 54]. Исходя из приведенной точки зрения, при рассмотрении криминалистической характеристики отдельного вида или группы преступлений представляется необходимым характеризовать способы подготовки, совершения и сокрытия преступления по раздельности, а не как единый структурный элемент.

К способам подготовки к совершению хищений в сфере оборота криптовалют можно отнести следующие:

1. Подбор технических средств и устройств, пригодных для создания вредоносных программ, фишинговых сайтов и обеспечения непрерывного доступа к сети Интернет, способных по своим функциональным характеристикам помочь киберпреступникам в реализации преступного замысла (компьютеры всех типов, видеокарты, флеш-накопители, роутеры, модемы и т. д.).

2. Приобретение (покупка готовых либо заказ по специальным требованиям) или создание вирусных программ и программ, обеспечивающих удаленное считывание информации со стороннего устройства, программного обеспечения для создания фишинговых сайтов, ICO- и SCAM-проектов.

3. Предварительное обучение, характерное для преступников, не обладающих специальными знаниями в области программирования, криптографии и иных отраслей IT-индустрии, необходимыми для реализации выбранных способов совершения хищений в сфере оборота криптовалют. При этом обучение и подготовка могут проходить как в самостоятельном порядке путем изучения соответствующих тематических форумов (где уже состоявшиеся киберпреступники зачастую делятся своим удачным опытом, представляют «рабочие» схемы, раскрывают лазейки в программных кодах различных криптоплатформ и т. д.), просмотра видеороликов, общения с практиками в группах социальных сетей, так и под руководством иных лиц, обладающих необходимой специализацией (посещение либо покупка обучающих курсов, тренингов, участие в семинарах, вебинарах и т. д.).

4. Подбор соучастников и распределение ролей между ними. Для хищений криптовалют характерным признаком является совершение преступлений либо группой лиц по предварительному сговору, либо организованной преступной группой, реже встречаются единичные исполнители. Решение о подборе соучастников может быть стихийным, т. е. возникшим случайно при определенных сложившихся обстоятельствах, либо запланированным, когда поиск участников осуществляется целенаправленно, исходя из отведенной каждому члену группы роли.

5. Сбор информации о лицах, в отношении которых планируется совершение хищений в сфере оборота криптовалют (преимущественно через ресурсы сети DarkNet). К такой информации можно отнести паспортные данные, ID и пароли от криптокошельков, сведения о владельцах криптокошельков, логины и пароли от аккаунтов электронной почты, социальных сетей, мессенджеров, реквизиты банковских карт и другие.

6. Выбор способа анонимизирования личности преступника через сокрытие IP-адреса устройства, что позволяет осуществлять различную деятельность в сети Интернет скрыто от провайдера и правоохранительных органов. С целью минимизации количества цифровых следов, которые могут быть оставлены киберпреступником при совершении хищений в сфере оборота криптовалют, последние

пользуются возможностями различных сервисов-анонимайзеров и IP-телефонией. К таким сервисам можно отнести VPN-сервер, прокси-сервер SOCKS, TOR-маршрутизатор, механизмы маршрутизации NAT и DHCP.

Способы совершения хищений в сфере оборота криптовалют целесообразно разделить на три группы в зависимости от вида совершаемого хищения.

1. Способы совершения вымогательства:

1.1. Путем распространения вирусных программ, блокирующих работу устройства или отдельных его программ. Вирусы-вымогатели можно классифицировать по нескольким основаниям:

1) в зависимости от программного кода, специфики его проникновения и работы на устройствах выделяют «сетевых червей» с функциями трояна, троянские программы и хакерские утилиты;

2) в зависимости от способа воздействия на процесс работы «зараженного устройства»: вирусы, блокирующие работу компьютера в целом (блокируется рабочее окно, и пользователь не может осуществить какие-либо действия в операционной системе), блокирующие работу только определенных программ (в большинстве случаев это программы пакета Microsoft Office); вирусы, шифрующие содержимое файлов (характерно для текстовых файлов, а также баз данных и таблиц Excel); вирусы, имитирующие работу антивирусных программ (такое программное обеспечение информирует пользователя об обнаруженных опасных вирусах, угрожающих повреждением хранящейся на устройстве информации, для удаления которых требует внесения платы в криптовалюте, в противном случае устройство подлежит блокированию);

3) в зависимости от типа устройств, на которые внедряются: вирусы, функционирующие на компьютерах с различным типом операционной системы (DoppelPaymer, Pay2Key, Regret Locker, Ragnar Locker, Ryuk); вирусы, предназначенные для дезорганизации работы мобильных устройств и планшетов (CovidLock).

Среди способов распространения вирусов-вымогателей в сети Интернет можно выделить отправку зараженных файлов или активных ссылок, автоматически запускающих скачивание вируса, через спам-рассылку, всплывающую рекламу, посредством электронной почты, мессенджеров и социальных сетей, загрузку вируса при посещении небезопасных сайтов.

1.2. Путем хищения личных данных пользователей через взлом аккаунтов социальных сетей, который возможен несколькими способами: путем подбора пароля или его смены через электронную почту, перехваченные СМС-сообщения; путем распространения вирусов и расширений для браузеров, тесно контактирующих с социальными сетями и требующих от пользователя подтверждения такого взаимодействия; путем перехвата пароля через открытые точки доступа Wi-Fi.

1.3. Путем «пылевой атаки» (dusting attack) на криптокошельки. Движение определенной публичной криптовалютной единицы от одного кошелька к другому можно отследить с помощью анализаторов. Такая возможность привела к новому виду вымогательства — «пылевой атаке», где под «пылью» понимают наименьшее возможное количество определенного вида криптовалюты, направляемое вымогателем случайному пользователю, с целью анализа совершаемых последним транзакций с иными участниками и установления его личности через связь с криптобиржами и обменниками.

2. Способы совершения мошенничества:

2.1. Мошенничество, связанное с осуществлением гражданско-правовых сделок в сфере оборота криптовалют (потребительское). К потребительскому мошенничеству следует относить хищения криптовалют при совершении сделок по купле-продаже товара за криптовалюту, по сдаче в аренду помещений, техники, автомобилей и т. д., по обмену криптовалют на фиатные денежные средства или иные виды криптовалют.

2.2. Мошенничество в области инвестирования в SCAM-проекты и участия в деятельности SCAM-ресурсов. SCAM-ресурсы представлены многочисленными розыгрышами и лотереями, которые предлагают своим участникам либо выиграть популярные виды криптовалют за незначительную плату, являющуюся «взносом», либо поучаствовать в розыгрыше дорогостоящих товаров (автомобилей, турпоездок, смартфонов и т. д.), выиграв которые необходимо заплатить организаторам минимальный процент в криптовалюте для оформления подарка. Нередко в качестве SCAM-ресурса выступают распродажи и акции, организуемые от имени хорошо зарекомендовавших себя криптобирж и обменников.

SCAM-проекты представляют отрасль криптовалютных инвестиционных проектов, направленных на привлечение ресурсов вкладчиков под предлогом их планомерного циркулярного увеличения по мере раскрутки финансируемого проекта. Однако SCAM-проекты, в отличие от добросовестных инвестиционных ICO-проектов, не нацелены на реализацию поставленных задач и имеют заведомо преступную направленность. Объединяющим признаком для всех SCAM-проектов выступает способ прекращения преступной деятельности, который имеет две разновидности: либо полное уничтожение проекта, либо его «заморозка». При ликвидации проекта мошенники после вывода похищенных средств уничтожают любую информацию о нем, удаляют веб-страницы, рекламные объявления и т. д. В случае «заморозки» мошенники представляют своим инвесторам причину, по которой проект больше существовать не сможет. Среди часто встречающихся причин выделяются: хищение средств неизвестными хакерами; ошибки и противоправные действия сотрудников, работавших над проектом и имевших доступ к средствам вкладчиков; возникшие технические сбои; преступные действия, допущенные партнерами проекта, а не самими создателями. Такое «перебрасывание» вины на других лиц позволяет мошенникам спустя некоторое время возобновить проект и осуществить уже отработанную схему повторно.

2.3. Мошенничество в сфере использования института гарантов криптовалютных сделок. К услугам гарантов прибегают пользователи криптоплатформ, работающих без использования смарт-контрактов, когда взаимоотношения между контрагентами строятся на взаимном доверии. Гарант выступает посредником, обеспечивающим осуществление условий сделки. Однако действия мошенников-гарантов заканчиваются на этапе получения криптовалют для временного хранения, которые они обращают в свою пользу, и больше гаранты не выходят на контакт со сторонами сделки.

2.4. Мошенничество в области криптовалютного кредитования может осуществляться несколькими путями, исходя из роли преступников в кредитных отношениях: ими выступают либо заемщики, либо инвесторы, либо кредитные сервисы. Мошенничество со стороны заемщиков проявляется при получении займов под залоговое обеспечение или кредитного плеча без намерения вернуть кредитные средства. Хищение криптовалют кредитными инвесторами характерно для обеспеченных кредитов, когда последние используют децентрализованные кредитные площадки лишь для поиска будущих заемщиков, с которыми в последующем формируют сделку без использования смарт-контракта и внесения суммы кредита в пул платформы. Получив залоговую сумму, инвестор отказывается от сделки и ликвидирует свое кредитное предложение. Преступная деятельность криптовалютных сервисов направлена в большей степени на средства кредитных инвесторов при разработке SCAM-проектов данного направления. Однако имеют место и случаи хищения залоговых взносов заемщиков, которые противоправно списываются из пула кредитного сервиса на мошеннические кошельки, а заемщикам объявляется о хакерской атаке на сервис, повлекшей потерю всех средств без возможности компенсирования, поскольку страхование залогов не предусмотрено.

3. Способы совершения хищений путем модификации компьютерной информации:

3.1. Путем несанкционированного доступа к криптокошелькам посредством использования фишинговых и фарминговых сайтов. Фишинговые и фарминговые сайты представляют собой поддельные веб-ресурсы, дублирующие (копирующие) страницы действующих криптосервисов с целью несанкционированного получения конфиденциальных данных пользователей, используемых для доступа к криптокошелькам с последующим хищением хранящихся в них криптовалют. Фишинговые сайты производят только внешнее дублирование реального ресурса, однако их URL-адрес имеет отличия в один или несколько символов от настоящего. В свою очередь, фарминговые сайты являются усложненной версией фишинговых и копируют не только дизайн ресурса, но и его индивидуальный адрес. Если для посещения фишингового сайта необходимо перейти по «активной» ссылке, доводимой до сведения потерпевшего через электронные письма, текстовые сообщения в мессенджерах, СМС-сообщения либо путем купленного у поискового сервиса рекламного места, то для привлечения пользователей на фарминговые сайты необходимо внедрение вредоносного программного кода, изменяющего IP-адреса веб-страниц на сервере DNS с реальных на подставные, либо на устройство пользователя, либо на сервер копируемого ресурса. Фарминговые коды могут попадать на устройство пользователя при скачивании различных файлов, программ, посещении небезопасных сайтов.

3.2. Схожие с фишинговыми и фарминговыми сайтами цели преследуют и программы-шпионы, внедряемые на устройства пользователей для получения конфиденциальных данных. Такое вредоносное программное обеспечение проникает на пользовательское устройство через скачиваемые из сети Интернет файлы (вложения из электронных писем и сообщений в мессенджерах), программы и мобильные приложения, загружается в фоновом режиме при посещении определенных сайтов, в том числе фишинговых, устанавливается с подсоединяемых переносных устройств. Механизм работы вируса-шпиона направлен на копирование файлов (выявляются преступником путем удаленного анализа данных устройства), содержащих конфиденциальные сведения (файлы, связанные с работой локальных «горячих» криптокошельков, истории браузеров, данные менеджера сохранения паролей и т. д.), либо отслеживание действий пользователя на устройстве и в сети Интернет в режиме онлайн. Полученные сведения используются преступниками для несанкционированного доступа к криптокошельку и вывода из него средств.

3.3. Хакерские атаки на криптовалютные сервисы (кошельки, биржи, обменники) связаны с обнаружением преступниками, обладающими профессиональными навыками в сфере программирования, уязвимостей в работе программного кода и обеспечении безопасности от стороннего вмешательства серверов таких ресурсов. Получив доступ к серверу, преступник имеет возможность распоряжаться работой сервиса, дестабилизировать и блокировать его деятельность, анализировать данные участников, распоряжаться пулом средств платформы.

3.4. Хищения криптовалют путем подделки QR-адресов криптокошельков связаны с внедрением преступников в отношения между сторонами сделки и изменением адреса криптокошелька получателя средств на подставной. Отслеживая переписку по электронной почте, преступник перехватывает сообщение с QR-адресом получателя средств и заменяет его на свой, произведя повторную отправку письма. Вторая сторона, не замечая подмены, производит оплату, отправляя средства на кошелек преступника. Замене подвергаются именно QR-адреса, поскольку представляют собой графическое изображение, сложное для восприятия и быстрого запоминания, в отличие от буквенно-числовой комбинации.

3.5. Использование криптовалютными сервисами двухфазной системы аутентификации для доступа к аккаунтам пользователей (кошельков, бирж и обменников) привело к образованию еще нескольких способов осуществления хищения: путем

сим-свопинга или переадресации сообщений. Для реализации хищения криптовалют через сим-свопинг преступникам необходимо первоначально получить сведения об ID криптокошелька или логин аккаунта на бирже / обменнике, после чего перевести номер мобильного телефона с сим-карты пользователя на свою. Чтобы получить новую сим-карту с необходимым номером, нужно обратиться к оператору и изложить причину замены. Если получение сим-карты возможно без личного присутствия абонента (через звонок оператору или его мобильное приложение), то новая сим-карта может высылаться по почте, направляться курьером или преобразоваться в e-sim (не имеет материального носителя). Однако большинство мобильных операторов не осуществляют замену сим-карт удаленно, только при личном присутствии абонента. В этом случае преступники могут рассчитывать только на недобросовестных сотрудников компании мобильного оператора, оказывающих им пособнические услуги за вознаграждение.

Еще одна возможность перехватить СМС-сообщения с кодом доступа к криптокошельку — установить переадресацию входящих сообщений с номера пользователя на номер преступника (используют безыменные сим-карты или оформленные на подставных / умерших / несуществующих лиц). Современные мобильные операторы предоставляют своим клиентам возможность самостоятельно и удаленно управлять подключенными услугами через личный кабинет, попасть в который можно через официальный сайт оператора или мобильное приложение. Получив доступ к личному кабинету, преступник подключает переадресацию на нужный ему номер, после чего реализует вход в криптокошелек пользователя и осуществляет незаконное списание средств.

3.6. Хищения криптовалют в сфере получения флеш-кредитов базируются на манипуляциях с протоколами блокчейна и ценового оракула, что позволяет искусственно изменять курс нужных видов криптовалют, похищая образующуюся разницу. Основная проблема, породившая возможность хищения криптовалют через флеш-кредиты, — использование различными криптосервисами в качестве основного источника одних и тех же анализаторов волатильности курсов криптовалют.

Как правило, способы сокрытия цифровых следов в сети Интернет продумываются и подбираются киберпреступниками еще на стадии подготовки к совершению хищений, о чем, к примеру, свидетельствует выбор средств сокрытия IP-адреса используемых ими устройств. Однако определенный комплекс задач по сокрытию преступления может быть реализован только на стадии после его совершения. Среди таких задач можно отметить следующие:

1. Очистка интернет-пространства от следов совершенного преступления, которая производится путем удаления из общего доступа фишинговых или фарминговых сайтов, информации об ICO- и SCAM-проектах, ресурсах рекламного характера, ликвидации аккаунтов в социальных сетях, мессенджерах и электронной почте, на сервисах-анонимайзерах и IP-телефонии, дистанционной деактивации внедренных на устройство пользователя вирусных программ, снятия с торгов дублирующих криптовалют и др.

2. Анонимизирование и/или вывод похищенных криптовалют и денежных средств. В случаях хищения криптовалют последние, как правило, пропускаются через сервисы криптомиксеров и переводятся на криптокошельки анонимных платформ, а в некоторых случаях и по несколько раз (т. е. сначала на один анонимный кошелек, потом на другой и т. д.). В дальнейшем такие криптовалюты либо выводятся через криптобиржи и обменники, либо оставляются преступниками для последующего накопления, либо реализуются в инвестировании и совершении сделок купли-продажи товаров или услуг. Фиатные денежные средства, полученные в результате совершения хищений в сфере оборота криптовалют, либо переводятся на банковскую карту, оформленную на подставное лицо (такие карты, как правило,

приобретаются на форумах в DarkNet), либо обмениваются на криптовалюту анонимных платформ через криптообменники и биржи, либо обращаются в электронные деньги.

Таким образом, изучение криминалистической характеристики способов подготовки, совершения и сокрытия хищений в сфере оборота криптовалют имеет практическую значимость для органов предварительного следствия и дознания, поскольку именно способ обусловливает выбор орудий и средств совершения хищений, характеризует типичную следовую картину для каждой конкретной ситуации, позволяет установить наличие у лиц, совершивших преступление, определенных профессиональных навыков, знаний и умений, а также причины и условия, повлиявшие на совершение преступлений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О развитии цифровой экономики [Электронный ресурс] : Декрет Президента Респ. Беларусь, 21 дек. 2017 г., № 8 : в ред. Декрета Президента Респ. Беларусь от 18.03.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2022.

2. Криминалистическое обеспечение деятельности криминальной милиции и органов предварительного расследования : учебник / Т. В. Аверьянова [и др.] ; под ред. Т. В. Аверьяновой, Р. С. Белкина. — М. : Новый Юрист, 1997. — 400 с.

3. Князьков, А. С. Криминалистическая характеристика преступления в контексте его способа и механизма / А. С. Князьков // Вестн. Том. гос. ун-та. — 2011. — № 1. — С. 51–64.

Поступила в редакцию 12.05.2022 г.

Контакты: galuzodi@mail.ru (Шнейдерова Дарья Игоревна)

Shneiderova D. I.

METHODS OF PREPARATION, COMMISSION AND CONCEALMENT OF THEFTS IN THE SPHERE OF CRYPTOCURRENCY TURNOVER: CRIMINALISTIC CHARACTERISTICS

The article is devoted to the criminalistic analysis of the method of committing theft in the sphere of cryptocurrency transaction as a fully structured phenomenon, including a triad of methods of preparing, committing and concealing crimes. The author pays attention to the fact that the legal consolidation of the property status of cryptocurrencies allows them to be considered in the mechanism of committing various types of theft as a subject of criminal encroachment, as well as a means of realizing criminal intent or hiding stolen funds, which also affects the target orientation of the method chosen by the criminal to commit theft. Among the methods of preparation, the author highlights the selection of necessary technical means, malicious software for blocking work or remote espionage of the victim's device, passing preliminary training, collecting information about persons contemplated for theft, the selection of accomplices and the distribution of roles, the choice of means of anonymizing the person on the Internet. The methods of commission are divided depending on the type of theft committed and are grouped as methods related to extortion, fraud, theft by modification of computer information. Methods of concealment are characterized by a set of actions to eliminate or conceal electronic digital traces, as well as anonymization or withdrawal of stolen cryptocurrencies and funds.

Keywords: *cryptocurrency, crypto wallet, theft, method, concealment, preparation, criminalistic characteristics, fraud, extortion, modification.*